REMARKS

Claims 1-33 are pending in the application. Claims 1-33 are rejected. In the present amendment, Applicants amend Claims 1, 5, 25 and 29.

Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Lee et al (US 4,484,027). Amended claim 1 is not anticipated by Lee. Lee does not teach "extracting data bits *randomly* [emphasis added] from said processed received signal." Thus, claim 1 is patentable. Claims 2-4 are patentable since they are dependent on patentable claim 1.

Claim 5 is rejected under 35 U.S.C. 102(b) as being anticipated by Epstein (US 5,517,567). Epstein does not teach "a random number selector subsystem for generating random numbers from data bits generated from random received signal characteristics that are extracted from a received signal using existing wireless phone hardware," as required by claim 5. Epstein does generate random numbers from data bits generated from existing wireless phone hardware, but Epstein does not generate "random numbers from data bits generated *from random received signal characteristics* that are extracted from a received signal using existing wireless phone hardware," as required by claim 5. In Epstein, the random numbers are generated internally within the Master 200. They are not generated from data bits from a received signal as required by claim 5; therefore, claim 5 is patentable. Claims 6-12 are patentable since they are dependent on patentable claim 5.

Claim 13, 16-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein (US 5,517,567) in view of Takahashi et al. (US 5,659,618). The Examiner states that "[i]t would have been obvious to person of ordinary skill in the art at the time invention was made to employ A/D converter disclosed by Takahashi with wireless device taught by Epstein" since "analog data must be converted to digital before encryption." In Epstein, the Master 200, which generates random numbers does not process analog signals; therefore, there is no motivation to employ an A/D converter. Thus, there is no motivation to combine Takahashi with Epstein. Consequently, the limitations of "an analog to digital converter for converting the received analog signal to

a received digital signal," and "converting the received analog signal to a received digital signal," of independent claims 13 and 18 are not met. Thus, independent claims 13 and 18 are patentable. Claims 16-17 are patentable since they are dependent on patentable claim 13. Claims 18-24 are patentable since they are dependent on patentable claim 18.

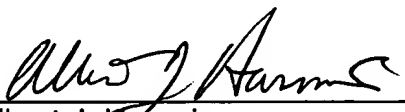
Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein (US 5,517,567) in view of Takahashi et al. (US 5,659,618) and further in view of Waldroup et al. (US 6,070,058). Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein (US 5,517,567) in view of Takahashi et al. (US 5,659,618) and further in view of Lee et al (US 4,484,027). As shown above there is no motivation to combine Takahashi with Epstein and since independent claim 13 is patentable, then dependent claims 14 and 15 are also patentable.

Claims 25-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes (Handbook of Applied Cryptography). The Examiner cited pages 171-172, section 5.2. The Examiner has not made a *prima facie* case of obviousness. "The prior art reference (or references when combined) must teach or suggest all the claim limitations" to establish a *prima facie* case of obviousness. Manual of Patent Examining Procedure, Eighth Edition, §706.02(j). Menezes does not teach or suggest all the claim limitations of claim 25. In fact, Menezes does not teach or suggest *any* of the claim limitations of claim 25. Thus, claim 25 is patentable. Claims 26-33 are patentable since they are dependent on patentable claim 25.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: February 24, 2003 By: 

Albert J. Harnois
Reg. No. 46,123
Attorney for Applicant

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 651-4368
Facsimile: (858) 658-2502

APPENDIX A

Page 5, The Paragraph beginning with the words "FIG. 2 illustrates..."

FIG. 2 illustrates a simplified partial signal path within a common CDMA phone receive hardware apparatus. **FIG. 2** shows the path of the signal only through the hardware used by the invention to generate random data.

Page 5, The Paragraph beginning with the words "Random Number..."

Random Number Selector Subsystem **214** is comprised of digital shift registers, which generate a new random number each time they are fed with new random bits and shifted. In the exemplary embodiment, the action of feeding and shifting occurs every 20 milliseconds. It will be understood by one skilled in the art that the principles described can be used to provide random bits at other time intervals. A new random number is supplied to Encryptor element **218** every 20 milliseconds.

Page 6, The Paragraph beginning with the words "FIG. 3 illustrates..."

FIG. 3 illustrates the apparatus employed in the exemplary embodiment of the present invention to generate 2 random bits of data from the demodulated digital receive signal input to the Receive AGC **208** every 20 milliseconds. Element **302** illustrates the received I/Q data input path passing to the AGC circuit. I/Q data refers to the In phase and Quadrature phase data samples produced by Quadrature Phase Shift Keying (QPSK) demodulation. The AGC circuit functions to provide a constant energy signal for demodulation. In so doing, AGC **208** produces a random variable intermediate output, known as a Receive AGC Adjusted bits (RX AGC ADJ) **310,** from the raw chip level input I/Q samples **302**. In CDMA technology, time is often measured in units of chip. Where CDMA frequency is 1.2288MHz, 1 chip = 1/(1.2288MHz) = 813.8 nanoseconds.

Page 6, The Paragraph beginning with the words "FIG. 3 illustrates..."

FIG. 3 illustrates the apparatus employed in the exemplary embodiment of the present invention to generate 2 random bits of data from the demodulated digital receive signal input to the Receive AGC **208** every 20 milliseconds. Element **302** illustrates the received I/Q data input path passing to the AGC circuit. I/Q data refers to the In phase and Quadrature phase data samples produced by Quadrature Phase Shift Keying (QPSK) demodulation. The AGC circuit functions to provide a constant energy signal for demodulation. In so doing, AGC **208** produces a random variable intermediate output, known as a [the] Receive AGC Adjusted bits (RX AGC ADJ) **310,** from the raw chip level input I/Q samples **302**. In CDMA technology, time is often measured in units of chip, where [. Where] CDMA frequency is 1.2288MHz, 1 chip = 1/(1.2288MHz) = 813.8 nanoseconds.

APPENDIX B

1. (Amended) A method for generating random data bits in wireless communications device, comprising the steps of:

processing a received signal; and

extracting [said random] data bits randomly from said processed receive signal.

5. (Amended) An encryption system, comprising:

a random number selector subsystem for generating random numbers from data bits generated from random received signal characteristics that are extracted from [the] a received signal using existing wireless phone hardware; and

an encryptor for encrypting a signal using said random numbers.

25. (Amended) A method for generating a continuous pool of mathematically random data for wireless communications encryption, comprising:

generating random data bits from an automatic gain controller and adding the bits to [the] a random data pool;

generating random data bits from a DC Offset Correction Loop and adding the bits to the random data pool; and

generating random data bits from a Time Tracking Loop and adding the bits to the random data pool.

29. (Amended) A wireless device for generating, from a received signal, a continuous pool of mathematically random data for wireless communications encryption, comprising:

an Automatic Gain Controller for generating random data bits to be added to [the] a random data pool;

a DC Offset Correction Loop for generating random data bits to be added to the random data pool; and

a Time Tracking Loop for generating random data bits to be added to the random data pool.